RECEIVED
CENTRAL FAX CENTER
JUN 23 2008

DILLON YUDELL LLP

ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
Examiner Turchen	Eustace P. Isidore, Reg. No. 56,104
ORGANIZATION: US Patent and Trademark Office	DATE: June 23, 2008
ART UNIT: 2139 / CONFIRMATION NO.: 8466	TOTAL NO. OF PAGES INCLUDING COVER:
FAX NUMBER: 571-273-8300	APPLICATION SERIAL NO.: 10/749,261
ENCLOSED: Compliant Appeal Brief	ATTORNEY DOCKET NO.: RPS920030206US2

☐ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 571 -273-8300 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Eustace P. Isidore *Date:* June 23, 2008 *Signature:*

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application Of:	§	**Atty. Docket No. RPS920030206US2**
	§	
RYAN CHARLES CATHERMAN	§	**Examiner: TURCHEN, JAMES R.**
	§	
Serial No.: 10/749,261	§	**Art Unit: 2139**
	§	
Filed: DECEMBER 31, 2003	§	**Conf. no.: 8466**
	§	
For: METHOD FOR SECURELY CREATING AN ENDORSEMENT CERTIFICATE UTILIZING SIGNING KEY PAIRS	§	

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Compliant Appeal Brief is submitted in response to the Notice of Non-Complaint Appeal Brief mailed on May 21, 2008, having a shortened statutory period, set to expire on June 21, 2008. No fee is believed to be required to submit this Brief. However, in the event any fees are required, please charge **IBM CORPORATION'S Deposit Account No. 50-0563.** No extension of time is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application to **IBM CORPORATION'S Deposit Account No. 50-0563.**

RECEIVED
CENTRAL FAX CENTER
JUN 23 2008

STATUS OF CLAIMS

Claims 1-6, 8, 10-22 and 24 stand finally rejected by the Examiner as noted in the Final Office Action dated August 16, 2007. Claims 7, 9, 16, 23 and 25 are canceled. The rejection of Claims 1-6, 8, 10-22 and 24 is appealed.

SUMMARY OF THE CLAIMED SUBJECT MATTER

As recited by Appellants' example method Claim 1 (and similarly configured system Claim 17), Appellants' invention provides a method (FIGs. 4 and 5) for securely creating an endorsement certificate for a device in an insecure environment. The method comprises: generating for a valid device (FIG. 2) an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable (¶¶ 0036, 0039; FIG. 4, 403); creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among: expiration of a preset amount of device manufacturing time; and manufacture of a preset number of devices from the plurality of valid devices (*see* ¶ 0040, 0041). The method further comprises: verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (*see* ¶ 0045, 0046; FIG. 4, 415, 416); and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device (*see* ¶ 0046, 0047; FIG. 4, 417, 419, 421; *see* also FIG. 5, ¶¶ 0049-0051). The signing key pair is a single-use parameter (¶ 0044), and the method further comprises immediately destroying said signing key pair within said device following a creation of said endorsement key (EK) (¶ 0044).

Appellants' Claim 12 further provides a data processing system comprising: a processor 150; a trusted platform module (TPM) chip 150; a bus for interconnecting said processor and said TPM chip; a network interface with communication means for connecting said TPM to a secure credential server 107; and means, whereby said TPM 150 is able to verify an endorsement key (EK) pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture (103) of the TPM, wherein said signing key pair is a single-use parameter (¶ 0044), said data processing system further comprising means for immediately destroying said parameter within said device following a creation of the EK (¶ 0044).

As provide by Appellants' Claim 13, the signing key pair has an associated signing key certificate that is sent to the secure credential server during manufacture of the TPM (¶ 0045). The means for verifying an endorsement key pair further comprises: means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed (EK) (¶¶ 0045-0046); and means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate (¶¶ 0045-0047; FIG. 4; *see* also FIG. 5, ¶¶ 0049-0051).

Similarly, Claim 14 provides a data processing system 104 utilized for issuing endorsement certificates. The data processing system 104 comprises: a processor; a memory couple to said processor via an interconnect; a security mechanism for ensuring optimum security of processes within said data processing system; input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key. Further, the data processing system comprises program means for: determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices; recording when a request for EK certificate fails

(FIG. 4, 423; ¶ 48; *see* also FIG. 5, ¶¶ 0049-0051); tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and messaging said TPM vendors to update their security procedures (*id.*).

Finally, Appellants' system Claim 17 (having similarly elements with Appellants' Claim 1) provides a system (FIG. 1) for securely creating an endorsement certificate for a device in an insecure environment. The system comprises: means for generating for a valid device (FIG. 2) an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable (¶¶ 0036, 0039; FIG. 4, 403); means for creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined system selected from among: expiration of a preset amount of device manufacturing time; and manufacture of a preset number of devices from the plurality of valid devices (*see* ¶ 0040, 0041). The system further comprises: means for verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (*see* ¶ 0045, 0046; FIG. 4, 415, 416); and means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device (*see* ¶ 0046, 0047; FIG. 4, 417, 419, 421; *see* also FIG. 5, ¶¶ 0049-0051). The signing key pair is a single-use parameter (¶ 0044), and the method further comprises immediately destroying said signing key pair within said device following a creation of said endorsement key (EK) (¶ 0044).

RECEIVED
CENTRAL FAX CENTER
JUN 23 2008

REMARKS

Appellants have pointed out with specificity the manifest error in the Examiner's rejections and the claim language which renders the invention patentable over the primary reference and the various combinations of references. Appellants, therefore, respectfully request that this case be remanded to the Examiner with instructions to issue a Notice of Allowance for all pending claims.

Respectfully submitted,

Eustace P. Isidore
Reg. No. 56,104
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS